MARSH & McLENNAN COMPANIES | Asia Pacific Risk Center

CYBER EVOLUTION

En Route to Strengthening Resilience in Asia-Pacific

FireEye

WHITE PAPER

CONTENTS

AUTHORS

Jaclyn Yeo
Senior Research Analyst
MMC Asia Pacific Risk Center
jaclyn.yeo@mmc.com

Rob van der Ende
Vice President, Asia Pacific & Japan
Mandiant, a FireEye Company
rob.vanderende@mandiant.com

CONTRIBUTORS

FireEye
Bryce Boland
Vivek Chudgar
Patty Hullinger
Patrick Neighorn
Tony Sapienza
Lynn Thorne
Timothy Wellsmore

Marsh & McLennan Companies
Matthew McCabe, Marsh, US
Stephen R Vina, Marsh, US
Richard D Green, Marsh, Asia
Douglas Ure, Marsh Risk Consulting, Asia
Kelly Butler, Marsh, Australia
Leslie Chacko, MMC Global Risk Center
Wolfram Hedrich, MMC Asia Pacific Risk Center

Knowing no boundaries, cyber incidents or data fraud and thefts that originate from North America or the European continent **quickly impact APAC**.

Executive Summary

The cyber threat landscape is morphing constantly and dramatically. Around the world, cyber dependency grows as increasing digital interconnection among people, things, and organizations expand. Asia-Pacific (APAC) is no different.

Knowing no boundaries, cyber incidents or data fraud and thefts that originate from North America or the European continent quickly impact APAC, inflicting significant financial and personal data losses, as well as severe business interruptions. These compound the effects of information infrastructure and network failures.

Beyond currency volatility to political instability and evolving regulations, conducting business across borders today involves more risks – and companies must add cyber to their list of risk concerns. Financial services, energy and utilities, and telecommunications are among the most-investigated industries in APAC, highlighting the urgent need for higher awareness levels, stronger mitigation measures, and improved cybersecurity postures.

Cyber challenges in APAC, such as low cybersecurity investments and long dwell times, can be attributed to the complex geopolitical tensions, exposed critical infrastructure, and the severe shortage of cybersecurity talents in the region.

Fortunately, the regulatory climate in APAC is changing – slowly but surely. Although most APAC countries today are not legally obliged to report any cyber incidents and many remain silent, countries such as Singapore and Australia already have plans to adopt mandatory breach notification laws in 2018. The sooner governments and businesses recognize today's cyber landscape poses a top enterprise risk, the better prepared they can be to take active steps to address the inevitable breach.

As trusted cyber advisers, FireEye and Marsh & McLennan Companies – each a leader in its own field – have collaborated to produce this white paper to help organizations across APAC build and strengthen their enterprise cyber resilience.

The shifting cyber threat landscape across Asia-Pacific

Cyber criminals and other threat actors with malicious intent are more sophisticated than ever, finding new and inventive ways to carry out attacks. Globally, more companies have accepted this reality and are proactively protecting themselves against cyber attackers. In general, companies are more likely to adopt a posture of continuous cybersecurity.[1]

The growing interconnectedness between both digital and physical worlds and the increasing dependence on IT systems has exponentially expanded the surface areas for cyber attacks. This, coupled with the rising sophistication by cyber criminals, has evolved to become a major risk for enterprises and society. Besides dramatically increasing the value of information stored on network systems, the growing digital connectivity of people, things, and companies has given rise to more frequent cyber attacks, data fraud and theft, and compounded the effects of information infrastructure and network failure.

What does this mean for the APAC region?

The APAC region, which typically includes much of East Asia, South Asia, Southeast Asia, and Oceania, is heterogeneous and differs widely in terms of cybersecurity commitments and preparedness. According to the Global Cybersecurity Index 2017,[2] Singapore topped the world ranking in terms of its commitment to raise cybersecurity awareness, together with several APAC countries that scored relatively high on the index: Malaysia (3rd), Australia (7th), Japan (11th), and South Korea (13th). However, other key populous economies in Asia did not fare as well, such as India, China, and Indonesia, which ranked 23, 32, and 70 respectively.

Countries in APAC, in general, have fared relatively badly in dealing with these cybersecurity disruptions due to lower cyber awareness levels. The reasons for this are shown in Figure 1.

[1] The cybersecurity posture of an organization refers to its overall cybersecurity strength, relating to the Internet and the vulnerability to the external threats.
[2] BRINK News 2017. Singapore tops global cybersecurity index.

Figure 1. Key attributes for low cyber awareness and insurance

LEGACY SYSTEMS

Long-standing business processes pose resistance to change

- Risk management often kept in-house
- Inertia towards allocating additional resources (i.e. time, budget) to cybersecurity technologies

LACK OF NECESSITY

Inadequate regulations and legislation

- Apparent lack of urgency and severity
- No single standardized cybersecurity protocol or notification requirements for businesses to adhere

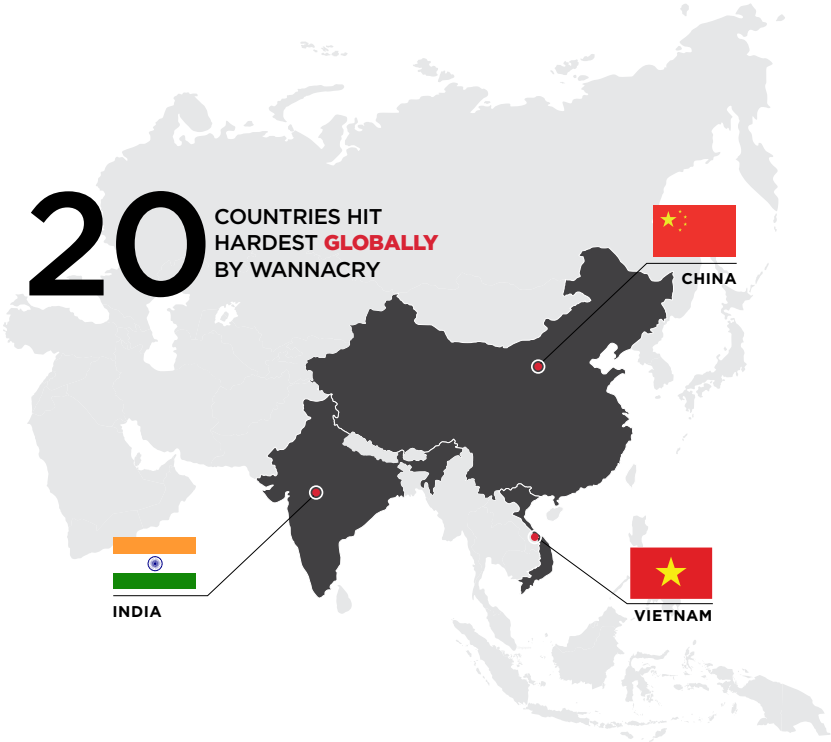
LACK OF GOOD QUALITY DATA

Limited good quality actuarial data

- Challenge in measuring cyber risk exposure
- Lack of cybersecurity maturity and readiness
- Often over-priced cyber insurance with excess coverage that does not mitigate the risk effectively

(**Source:** Asia Pacific Risk Center (APRC) analysis)

The Asia-Pacific (APAC) region, which typically includes much of East Asia, South Asia, Southeast Asia, and Oceania, is heterogeneous and **differs widely in terms of cybersecurity commitments and preparedness**.



APAC still has the highest dwell times due to a basic lack of investment in appropriate cybersecurity measures.

Companies across the region can improve their cybersecurity in many ways. One crucial measure — dwell time — indicates that, in general, APAC companies lag well behind their global counterparts. Dwell time statistics (Figure 2) — the amount of time (in days) between network intrusion and the detection of the threat actor — is highest in APAC when compared to the global average, as well as the statistics in the Americas, and Europe, Middle East, and Africa (EMEA).

The typical time between an attacker compromising a secured network and the breach being detected (reported by FireEye as "median dwell time" in its annual M-Trends report[3]) amounted to 172 days in the APAC region during 2016. This is almost twice as long as the global median dwell time of 99 days in the same year. This indicates cyber criminals, on average, spend almost half a year undetected within the compromised network — assessing and stealing valuable data and disrupting critical operations before they are discovered.

The decreased dwell time in APAC from the previous year might be considered an improvement that is only partially attributed to better testing methodologies[4] (such as Red Teaming and Response Readiness Assessments to proactively understand security postures).

Attacks that are identified quickly — like ransomware and destructive wiper attacks — skew these statistics, but the difference is due to the changing nature of the attacks, and not the cybersecurity measures in place. APAC still has the highest dwell times due to a basic lack of investment in appropriate cybersecurity measures.

Moreover, the ever-evolving cyber risk landscape and lack of best practices around managing cyber risk posture further exacerbate these attacks. The threat of large cyber attacks has significantly increased in importance in 2017, according to the World Economic Forum's 2017 Executive Opinion Survey,[5] an exclusive poll in which 12,400 executives across 136 countries identified the global and regional risks of highest concern for doing business in their countries.

Cyber risks have historically been among the top five risks for executives in East Asia and the Pacific, but the various high-profile cyber attacks in 2017 have prompted executives to pay closer attention to the potential damage these attacks may cause. Most notable among these incidents is the WannaCry ransomware attack in May 2017 that severely disrupted businesses in major Asian economies, with China, India and Vietnam reported to be among the 20 countries hit hardest globally.

[3] FireEye, 2017. M-Trends 2017: A View from the Front Lines.
[4] BRINK News, 2017. Singapore tops global cybersecurity index.
[5] BRINK News, 2017. Politics and cyber are rising concerns for business leaders.

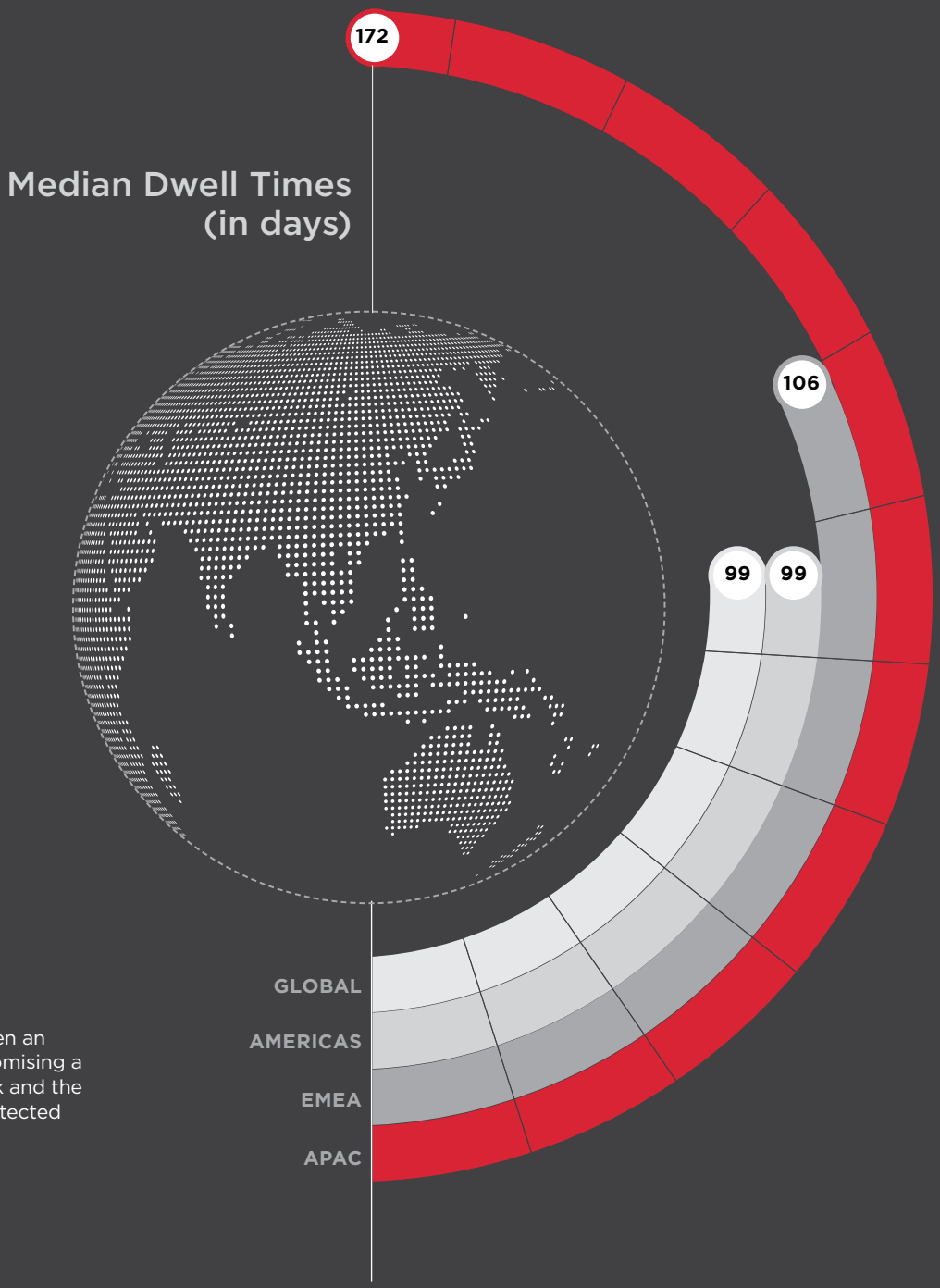


Figure 2. Asia-Pacific continues to report the world's highest dwell times

(**Source:** APRC analysis; FireEye M-Trends 2017)

Cyber attacks with financial motivations were perceived as the top cyber threat for global corporations across industry sectors in APAC.

Recent cyber trends in Asia-Pacific

39%

Financial motivation is perceived as the top threat for global corporations doing business in APAC

54%

Insider threats - from errors to access - are the second biggest concern among companies operating in APAC

According to the global Marsh/Microsoft Global Cyber Risk Perception Survey 2017 administered between July and August 2017, cyber attacks with financial motivations were perceived as the top cyber threats for international corporations across industry sectors in APAC (39 percent). With extortion for financial gain the key goal of stealing insider information or confidential intellectual property, (see Figure 3), it is reasonable to expect that inventive cyber attack techniques will continue to emerge and evolve in the cyber risk landscape.

Companies operating in APAC are also concerned about insider threats on the whole. Respondents ranked employees or contractors with malicious intent, human error, third-parties with access to the network systems, and operational errors as the next biggest threats (54 percent).

Q: With regard to a cyber attack that delivers destructive malware, which threat actor concerns you?

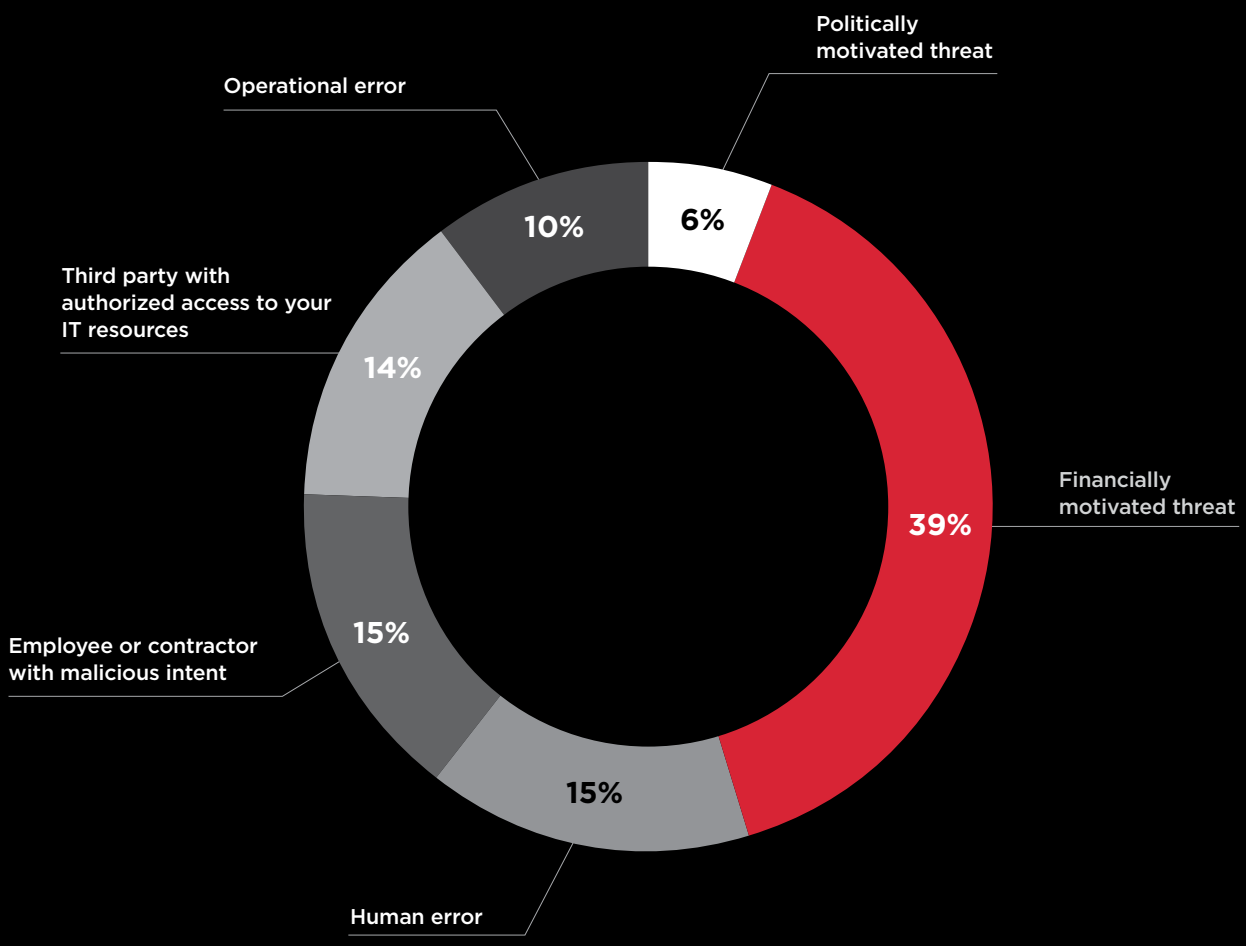


Figure 3. Survey of corporations' views on the top cyber threats when doing business across Asia-Pacific

(**Source:** APRC; dataset from Marsh/Microsoft Global Cyber Risk Perception Survey)

Estimating the financial cost of Wannacry global ransomware

Global financial and economic loss estimates from the WannaCry attack that crippled systems across at least 150 countries[7] range between hundreds of millions to $4 billion, making it one of the most damaging incidents involving so-called "ransomware," in which data from infected computers is encrypted and a cryptocurrency ransom payment is demanded for decryption of the data.

The attack is likely to make 2017 the worst year for ransomware scam victim organizations.

Similar schemes have resulted in losses of up to $1 billion annually,[8] according to market researcher Cybersecurity Ventures. They include lost productivity, the cost of conducting forensic investigations, and data restoration and recovery.

While the potential losses from reduced productivity and efforts to mitigate the damage from WannaCry are markedly significant, the actual ransom collected is modest by comparison, totaling approximately $150,000. During the early stages of the attack, it was found that ransom payments did not result in a decryption key being provided, leaving most victims to rebuild and recover from backups or other sources rather than pay the ransom.

Often, external threats result in the data breaches that grab news headlines. While these breaches are often costly, external threats can generally be addressed with traditional security measures, such as gap analysis, firewalls, device and endpoint encryption, and vulnerability and patch management. However, potential threats that originate from within the companies may often be more difficult to prevent, since they may unintentionally pose a threat to the internal network security. For example, some data breaches are due to human errors and are unintentional when someone falls for malicious phishing emails and clicks on infected links.

Regardless of how data breaches occur, to mitigate insider, outsider, intentional and unintentional threat risks, a more holistic approach to cybersecurity is essential in this evolving cyber threat landscape.

Globally, malicious external threats were the leading source of data breaches in the first half of 2017, as revealed by the latest breach level index.[6]

Figure 4 illustrates some of the most noteworthy data breaches and cyber incidents in the APAC region since June 2016.

[6] Gemalto, 2017. Poor internet security practices take a toll – Findings from the first half 2017 (Breach Level Index).
[7] CBS News, 2017. Cyberattack hit more than 100,000 groups in at least 150 countries, Europol says.
[8] Cybersecurity ventures, 2017. Cybercrime Report 2017 Edition.

2017 notable breaches and cyber incidents in Asia-Pacific

Global ransomware - Petya[13]
AUSTRALIA (JUN 2017)

Several Australian businesses, including courier companies, transportation systems, and legal firms, were hit by a vicious global ransomware attack that demanded **$300**[14] in Bitcoin for each incident breach.

DDoS and business interruption[11]
SINGAPORE (OCT 2016)

Local telecommunications providers suffered a distributed denial-of-service (DDoS) attack on their domain name system, resulting in a service outage that disrupted internet connectivity amongst the **470,000** subscribers.

Phishing attacks by external actors[9]
AUSTRALIA (JUN 2016)

A large Australian firm suffered a significant breach from financially motivated cyber threat actors via phishing emails that targeted employees with access to financial systems. The attacker stole **AU$1.2 million**, but the actual total damage is estimated to be more than **AU$2 million**.

Global ransomware - WannaCry[12]
CHINA (MAY 2017)

More than **29,000** institutions were infected by the malware and **15%** of universities' internet protocol addresses were attacked. Other critical information infrastructure affected were railway systems, hospitals, and govenment services.

Installed malware and data breach[10]
S. KOREA (JUL 2016)

The South Korean government was demanded ransom (more than **US$2 billion**) after personal identifiable information was leaked due to illegally installed malware in a large online shopping site.

Figure 4. Notable Breaches in APAC from 2016 to 2017 (**Source:** APRC)

[9] M-Trends 2017, Page 40. APAC Notable Breaches, June 2016.
[10] M-Trends, Page 40. APAC Notable Breaches, July 2017.
[11] Channel News Asia, 2016. DDoS attack on StarHub first of its kind on Singapore's Telco.
[12] AP News, May 2017. The Latest: 29,000 Chinese institutions hit by cyberattack.
[13] ABC News, 2017. Petya cyber attack: Ransonware virus hits computer servers across globe, Australian office affected.
[14] Straits Times, 2017. Cyberattack reachs Asia and Australia as new targets hit by ransomware demand.

Highly targeted industries in Asia-Pacific

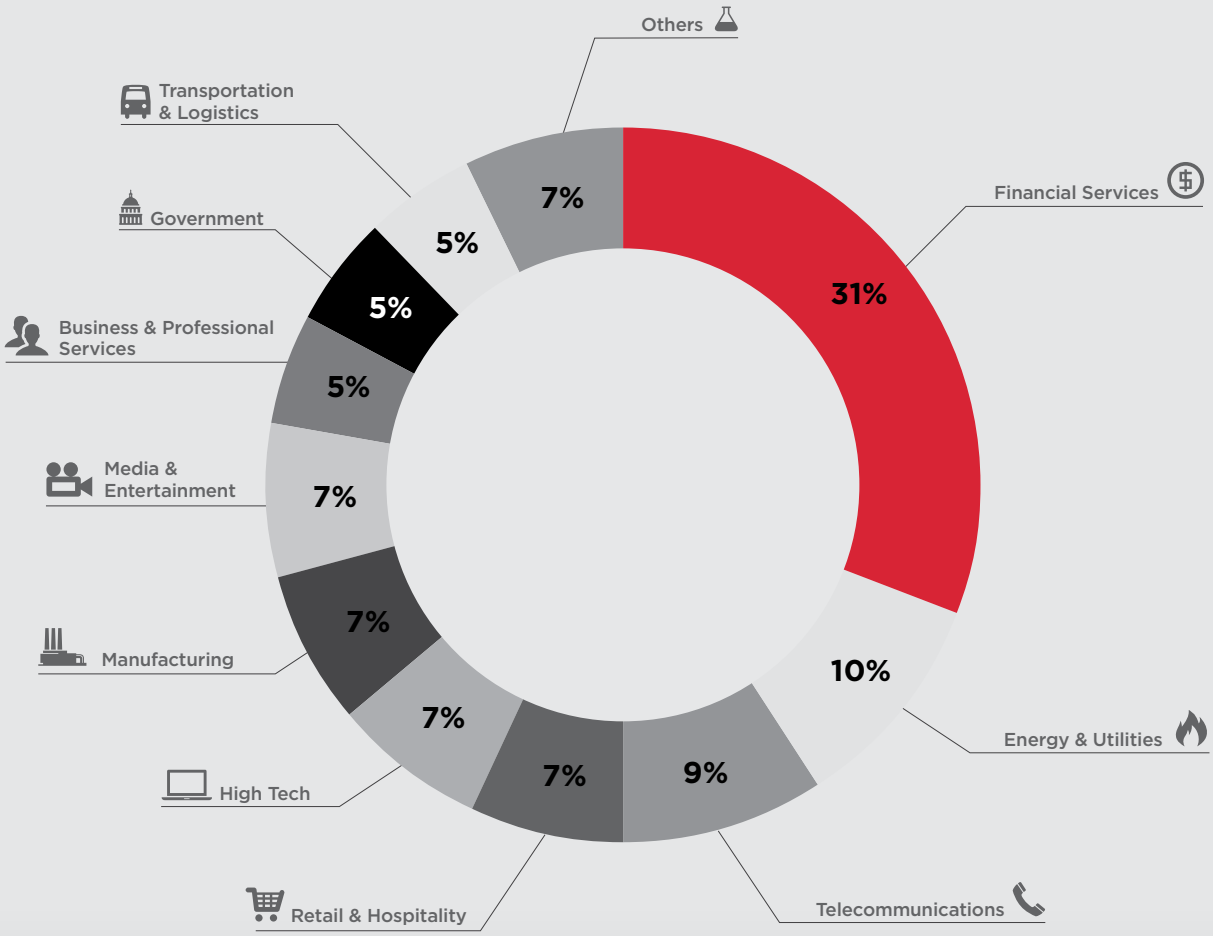
Conducting business internationally has always involved additional risks. Besides currency volatility, political instability and evolving regulatory climates, businesses must add cyber risks to their list of concerns.

According to FireEye, financial services recorded the largest share of FireEye clients (31 percent) investigated in cyber attacks, while the other sectors are almost equally at risk, each recording between 5 – 10 percent. (See Figure 5.)

31%

FireEye financial services clients targeted in cyber attacks

Figure 5. Percentage of FireEye investigations in Asia-Pacific by industry (**Source:** FireEye M-Trends 2017)



Others include:
Biotech & Pharmaceuticals, Healthcare, Construction & Engineering, and Non-profit

The following industries in the APAC region currently appear to be at particular risk for cyber intrusion:

FINANCIAL SERVICES

31%

Cyber crime is the greatest threat to the financial services industry. Victims often include a wide range of financial institutions, including banks, investment services, and insurance companies, among others. Developing trends in cyber crime include:

- Increases in attempted and successful exploitation of banks' client-side connections, such as those used for interbank payment services
- Exploitation of payment card industry information and protocols
- Use of malware to bypass multi-factor authentication

Cyber espionage is another significant threat to the industry; financial services have seen attackers using a higher-than-average number of watering holes — such as compromised third-party websites trusted by members of the finance industry — to deliver malware and profile targets while appearing to deliver legitimate traffic. Threat actors use economic cyber espionage to acquire intellectual property and sensitive information for long-term economic advantages, either for themselves or on behalf of their sponsors, which can include nation-states or business competitors.[15]

[15] FireEye, 2017. Target Cyber Criminals to Stop Cyber Crime.

ENERGY AND UTILITIES

10%

This industry faces cyber threats mostly from Advanced Persistent Threat (APT) groups that will likely attempt to steal IP to improve their state's domestic infrastructure, or provide an advantage in negotiations with foreign companies. In the event of conflicts, APT groups may seek to assist their sponsoring government by disrupting an adversary's energy supply and utility services, while interfering with its ability to provide its residents with essential public services.

Unlike cybercriminals intent on compromising organizations to steal and monetize clients' personally identifiable information, payment card information, and customers' credentials, attacks on the operational technology (OT) side of the industry focus primarily on disrupting systems such as industrial control systems that operate and control the generation and supply of fuel, electricity, and water. More notable and potentially far more severe, the OT side of this sector has seen threat levels increase significantly since 2014.

Attacks of this nature have far-reaching consequences that inconvenience a significant number of users. For example, in the 2015 Ukrainian utility attack, simultaneous localized power outages occurred across the country. This resulted in approximately 80,000 energy customers in one city enduring an outage for six hours,[16] while 125,000 energy customers in another city faced outages for two hours. Attackers appeared to be motivated mostly by geo-political agendas.

TELECOMMUNICATIONS

9%

The telecommunications industry today provides a wide array of global services that connect millions of customers around the world; this diverse business ecosystem faces increasingly frequent cyber risks.

APT groups target the telecommunications industry in particular, given its prominent role in our modern society today and its importance to both the civilian and military spheres. They may also seek to gain access to clients' networks, or conduct more traditional espionage activities related to surveillance. Other factors that may influence further targeting of the sector include:

- Greater numbers of linked devices and the Internet of Things to the telecommunications network significantly expose vulnerabilities and increase the surface area for attacks
- The development of new technologies and processes often attracts APT groups engaging in economic espionage to benefit their sponsoring country's domestic industry
- Disclosures regarding alleged involvement in espionage or surveillance may put telecommunications companies at risk of threats from hacktivists seeking to protest such activities and embarrass organizations involved

Across APAC, the three most-investigated industries — financial services, energy and utilities, and telecommunications — exemplify the urgent need for higher awareness levels, stronger mitigation measures, and improved cybersecurity postures. The share of targeted attacks in these industries is much lower in more cyber-mature regions such as the US, at 15, three and two percent, respectively.

Across APAC, the three most-investigated industries — **financial, energy and utilities, and telecommunications — exemplify the urgent need for higher awareness** levels, stronger mitigation measures, and improved cybersecurity postures.

[16] FireEye, 2017. Sandworm Team and the Ukrainian Power Authority Attacks.

Cyber risk perception in Asia-Pacific

While cyber is perceived as a top risk across APAC, this perception is inconsistent with the region's level of preparedness.

More than half (58 percent) of the global respondents across major industries from the Marsh/Microsoft Global Cyber Risk Perception Survey 2017 rank cyber as one of the top five risks; almost two-thirds (65 percent) of respondents from larger companies with annual revenues of more than $5 billion prioritize cyber as one of the top five risks under their company's risk register. Yet, quantifying cyber risk is a key roadblock businesses face.

The survey further revealed that more than half of the respondents doing business in Asia (54 percent) and Pacific (50 percent) either do not estimate or do not know whether they estimate the financial impact of a cyber incident. This suggests that their true cyber exposure remains unknown, and that these companies are unprepared for potential cyber attacks.

58%

Respondents who rank cyber as one of the top five risks

50%

Companies doing business in the Pacific that don't estimate the financial impact of a cyber incident

Quantifying cyber risk is a **key roadblock** businesses face.

Q: If your organization has estimated the financial impact of a cyber incident, what is the worst potential loss value?

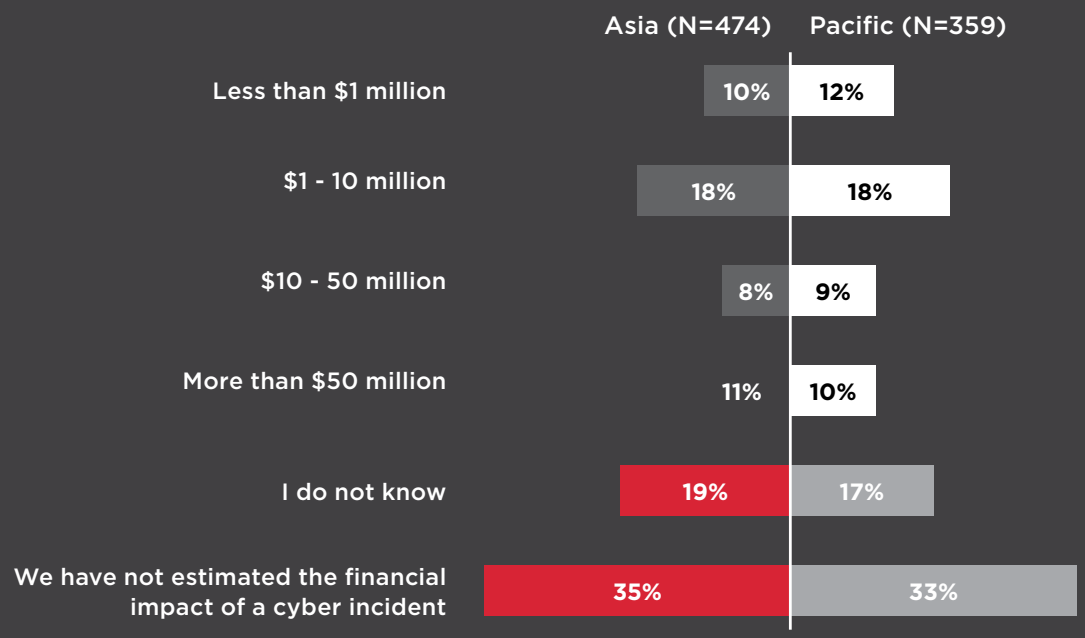


Figure 6. Perception of corporations' awareness of their organization's cyber risk exposure

(**Source:** APRC; dataset from Marsh/Microsoft Global Cyber Risk Perception Survey)

Key drivers of cyber challenges in Asia-Pacific

Several recent high-profile cyber attacks struck APAC and resulted in large-scale data and financial losses. Unsurprisingly, the most recent ransomware attack incurred significant costs in services and production disruptions as well as data recovery costs across the region.

The main causes for the region's susceptibility to attacks are the lack of transparency requirements, a weak cyber-regulatory environment, low investment in information security, and long dwell times, which are direct results of the low level of cyber preparedness in APAC.

In addition to having a cybersecurity landscape that is less mature than in other regions, APAC must overcome several cybersecurity hurdles to improve its defenses.

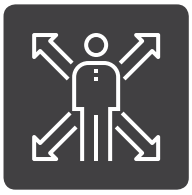
Geopolitical tensions

Asia-Pacific is home to numerous geopolitical conflicts. These conflicts create uncertainty for governments, which in turn creates demand for information, which fuels cyber espionage and other intelligence information. Cyber espionage operations are mostly aimed at collecting information to understand adversaries' tactics and capabilities, and to identify key decision makers. While government agencies are common targets, so are some private-sector organizations.

Exposed critical information infrastructure

No country today can credibly claim its entire critical information infrastructure (CII) system is well defended against cyber attacks. Cyber attacks against CII systems were not an important national consideration in most of APAC until recently, when attacks became more sophisticated with malicious intents. Thus, CII systems that manage utility plants, transportation networks, hospitals, and other essential services remain more vulnerable to increasingly frequent attacks. FireEye routinely observes state-linked offensive operations that could be part of forward military operations. Successful cyber attacks can adversely affect CII systems and disrupt essential services, in turn impacting business and consumer confidence levels.

Cybersecurity talent shortage



The worldwide spending on cyber defense products and services is forecast to exceed $1 trillion[17] from 2017 to 2021. The lack of human capital to drive these initiatives is another key roadblock. The global cybersecurity workforce continues to face a serious 1.5 million[18] talent shortage by 2020, amidst the recent cyber incidents, data breaches, and shifting industry dynamics and regulatory changes. As cyber risks become increasingly prevalent, companies must either find new recruitment channels, or raise and enhance awareness of cybersecurity among existing IT employees.

[17] Cybersecurity Ventures, 2017. Cybersecurity Market Report.
[18] Center for Cyber Safety and Education, 2017. Global information security workforce study 2017.

> Most APAC countries today are not legally obliged to report any cyber incidents **and many remain silent**.

Asia-Pacific's evolving regulatory climate

Limited information and disclosure regarding the scale and frequency of cyber attacks in the region may contribute to a false sense of security that could cost businesses dearly. Furthermore, most countries in Asia-Pacific today are not legally obliged to report any cyber incidents, and many remain silent—leading to the perception that cyber attacks are not as prevalent and severe as they truly are.

The transparency issue is further compounded by a lack of cybersecurity safeguards and standards. The collective result is that many companies in APAC are not aware of cyber risks and data breach consequences, underpinning the region's susceptibility to cyber attacks.

Even in the United States, where mandatory breach notification laws were first enacted in 2003, timing requirements for notifying affected parties have often been inadequate and ambiguous. Companies are only required to disclose a breach to customers "as soon as possible." By way of comparison, the proposed European General Data Protection Regulation mandates a breach notification within 72 hours.[19] Further, severe data breach incidents in the US recently have resurfaced the nation's cyber-legislation debate of the timing for disclosure, and has catalysed amendments to data-breach notification laws in several states to notify affected parties "without reasonable delay" and within 30 days.[20] In addition, the legal and operational processes for confirming identities to prevent fraud need to be rethought.[21]

Progress is being made, however — especially among APAC-region countries that recently adopted similar data breach notification regulations. (See Figure 7.) Companies should work closely with their legal counsel when developing data privacy and security programs to ensure compliance with existing and emerging requirements.

[19] InterSoft Consulting, 2017. Art. 33 GDPR Notification of a personal data breach to the supervisory authority.
[20] Congressman Jim Langevin, Sep 2017. Langevin reintroduces the Personal Data Notification and Protection Act. https://langevin.house.gov/press-release/langevin-reintroduces-personal-data-notification-and-protection-act
[21] Oliver Wyman, 2017. The Equifax data breach and its impact on identity verification.

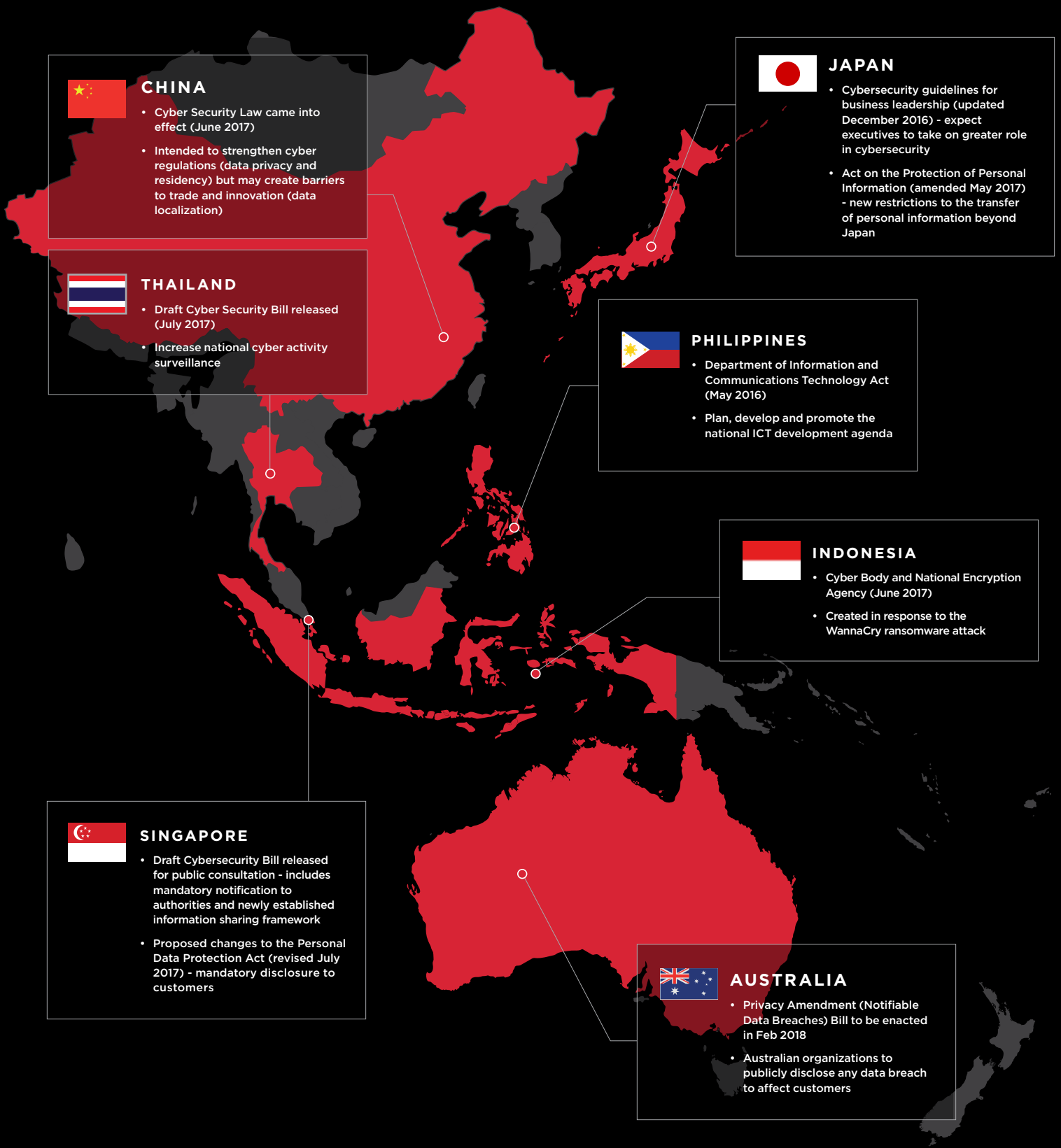


Figure 7. Recent regulations and their effect on companies doing business in APAC (**Source:** APRC analysis)

How companies can build cyber resilience

Cybersecurity investment

To keep pace with today's evolving threat landscape, companies should invest time and resources to examine their information security programs. This first requires understanding their business infrastructure and then identifying the cyber threat vectors that pose a risk to daily operations.

For example, a question such as, "What internal systems and data flows must be protected for the business to continue to function?" is crucial to preparing for an inevitable breach.

Recent cyber incidents are increasing in sophistication, and it is evident that companies need to conduct scenario analyses to be prepared for any possible outcomes.

However, as shown in Figure 8, preparation is only the first (crucial) step in building cyber resilience. Equally important is the focus on preventing as many threats as possible. Companies must have a contingency plan to quickly detect attacks and effectively respond to recover critical functions and minimize business interruptions.

For example, once key assets are identified, companies should prepare a security plan that links their technology to their associated cyber risk exposure. This enables the company to focus directly on protecting the technology, and in turn, the key assets. The ideal plan offers three benefits: visibility into the network to detect potential system intrusions; procedures for incident response; and adequate organizational capability to eradicate the attacker. This promotes good security hygiene and ensures vulnerabilities are not exploited. Comprehensive threat intelligence must also be leveraged to mitigate risk and improve the cybersecurity posture.

Business impacts of a breach do not typically occur immediately – it takes time for the attackers to map out the compromised network, steal what they are after, or damage the system. Companies with a heightened level of preparedness, detection-analytics, a proactive defense system, and critical response capabilities can disrupt the attack lifecycle before the full brunt of its impact is felt. These organizational readiness aspects should be tested and improved upon regularly through a combination of table-top exercises and 'live-fire' drills.

PREPARE	PREVENT	DETECT	RESPOND	RECOVER
Understand Cyber Risk Exposure	**Strengthen Internal Capabilities**	**Enhance Cyber Analytics**	**Manage Incident Impacts**	**Minimize Business Interruption**
• Industry and sector benchmarking exercises • Risk quantification, mapping and modelling • Proactive threat profiling (i.e. identifying their adversaries)	• Infrastructure protection and network security • Talent Management (i.e. attract and retain cybersecurity experts) • Proactive incident prep excercises (e.g. table-top exercise or wargames)	• Threat intelligence utilization • Vulnerability management	• Impact containment • Crisis management	• Incident response plans • Strategic risk transfer plans

Figure 8. Actionable strategies in maturing the cybersecurity posture (**Source:** APRC analysis)

Business disruption and the path to recovery

As demonstrated by the recent WannaCry and Petya ransomware attacks, resuming operations after a cyber incident is not as easy as switching the network back on.

Once a breach occurs, companies may find themselves in an extended period of outage while network forensics experts determine the extent of the breach and advise on the necessary remedies, action plans, and communication strategies for recovery. During that interim period, a temporary network is required to resume operations and minimize business interruption. In the meantime, affected customers should be briefed regularly to minimize damage to business reputation, while shareholders will want information on all attempts to mitigate potential revenue losses.

Remote access may also be disabled, incurring costs for remote employees who must temporarily move onsite to resume critical duties. Partial functionality may extend from days to weeks or even months, depending on the effectiveness of the business continuity management (BCM). Through a proactive and thorough assessment of the company's cyber risk profile, a bespoke cyber-business continuity plan (BCP) can address the company-specific cyber risks. As every system structure is different, a customized assessment and a plan for the company-specific loss profile are essential.

With appropriate resources focused on critical areas to develop an effective BCM, economic losses as a result of business interruptions, operational inefficiencies, and incremental out-of-pocket costs will likely be minimized.

Planning for the inevitable breach

What can you do now to prepare for a future cyber crisis? Cyber resilience depends on the company's ability to respond efficiently to a significant breach and continue operating effectively. In this regard (besides contingent planning), the transfer of residual cyber risks to the capital markets is also another key mitigation measure to consider.

The main role of insurance is risk transfer; and having recognized that cyber risk cannot be fully eliminated, companies must be prepared for an attack with adequate coverage.

Companies concerned about risk exposures from cyber disruptions need a better understanding of the potential insurable and non-insurable business values at risk, and possible recovery options. The Chief Information Officer and/or Chief Information Security Officer hold responsibility for much of this, including collaborating with cross-functional teams with buy-in from the board. Cybersecurity risks can also have a significant impact beyond technology – they can affect new business plans, capital investment decisions, mergers and acquisitions activities, product or service offerings, research and development processes, and many more.

For example, directors and officers perform this delicate balance and make prudent decisions under the scrutiny of external stakeholders. It is imperative that the board and its directors and officers commit time and resources to educate themselves and their employees on the ongoing and dynamic cybersecurity threats posed in this current digital and connected age.

As such, business leaders do not need to be "tech-savvy" to play an effective role in cybersecurity oversight. Just like any other business risk, it requires them to have an in-depth understanding of the company's business and strategy models, experience in leadership, sound business judgment, and more importantly, the ability to identify the risks to accept, avoid, or transfer through insurance.

This mindset shift is critical for understanding the potential costs and loss of income that may be caused by a cyber event. It can also assist an organization to make informed decisions about the appropriate level of cyber coverage, and the available coverage through property, crime, liability, or Directors and Officers policies.

From having a communications strategy in place to an incident response BCP, today's cyber landscape poses an enterprise risk that goes far beyond anything previously seen. The sooner governments and businesses recognize this, the better prepared they can be for the inevitable.

A Call to Action

FireEye and Marsh & McLennan Companies have collaborated on this white paper to provide an overview of the fundamental cyber challenges facing APAC and the appropriate risk management tools to address them. In light of the current cyber threat landscape, our goal is to increase awareness of the risk trends and recommend tangible steps for businesses and governments across APAC to protect against business interruption in the event of a cyber incident.

If you would like to learn more about cyber threats within the region, how to protect against them, and how to keep them from impacting your business enterprise, FireEye and Marsh & McLennan Companies are available to assist. Please contact us at cyberrisk@fireeye.com or https://www.marsh.com/us/services/cyber-risk.html.

About FireEye
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye minimizes the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 6,300 customers across 67 countries, including more than 40 percent of the Forbes Global 2000.

For more information, please contact cyberrisk@fireeye.com

About Marsh & McLennan Companies
Marsh & McLennan Companies (NYSE: MMC) is a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and people. As one of the four operating companies, Marsh is a global leader in insurance broking and risk management. As the world's most trusted cyber insurance broker, Marsh, Inc. advises over 1,000 clients regarding network security and privacy issues and has won Advisen's award for Cyber Broker of the Year in 2014, 2015 and 2016. With annual revenue of $13 billion and approximately 60,000 colleagues worldwide, Marsh & McLennan Companies provides analysis, advice and transactional capabilities to clients in more than 130 countries. The Company is committed to being a responsible corporate citizen and making a positive impact in the communities in which it operates.

For more information, please visit www.marsh.com/us/services/cyber-risk.html

About Asia Pacific Risk Center
Marsh & McLennan Companies' Asia Pacific Risk Center addresses the major threats facing industries, governments, and societies in the Asia Pacific Region and serves as the regional hub for our Global Risk Center. Our research staff in Singapore draws on the resources of Marsh, Guy Carpenter, Mercer, Oliver Wyman, and leading independent research partners around the world. We gather leaders from different sectors around critical challenges to stimulate new thinking and solutions vital to Asian markets. Our digital news service, BRINK Asia, keeps decision makers current on developing risk issues in the region.

For more information, please email the team at contactaprc@mmc.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
877 FIREEYE (347.3393)
info@FireEye.com

www.FireEye.com

FireEye